

## CLAIMS

What is claimed is:

1. A method for replacing a cryptology key in a computer module, wherein said computer module includes a plurality of evictable cryptology keys, said method comprising:

determining, for each of a plurality of evictable cryptology keys in a computer module, a replacement expense for each said evictable cryptology key, said replacement expense determined by:

a probability that each said evictable cryptology key will be needed by the computer module after said evictable cryptology key is evicted, and  
an amount of cycle time required to re-store, if evicted, each said evictable cryptology key in the computer module;

identifying a least expensive evictable cryptology key based on said replacement expense; and

replacing said least expensive evictable cryptology key with a replacement cryptology key.

2. The method of claim 1, said step of replacing said least expensive cryptology key further comprising:

locating a blob comprising said least expensive evictable cryptology key and a security software shell;

removing said security software shell from said blob; and

storing said least expensive evictable cryptology key in said computer module.

1           3.     The method of claim 1 further comprising:

2                 determining said cycle time by calculating a number of generations to a nearest  
3                 ancestor of said least expensive evictable cryptology key, said nearest ancestor being  
4                 from a plurality of non-evicted remaining cryptology keys in the computer module.

1           4.     The method of claim 3 further comprising:

2                 storing, if a parent cryptology key of said least expensive evictable cryptology key  
3                 is not stored in said computer module, a child cryptology key of said nearest ancestor key  
4                 of said least expensive evictable cryptology key; and

5                 repeating said storing step until said least expensive evictable cryptology key is  
6                 stored in said computer module.

7           5.     The method of claim 1, wherein the computer module is a Trusted Platform  
8                 Module (TPM).

1           6.     A data-processing system capable of replacing a cryptology key in a computer  
2     module, wherein said computer module includes a plurality of evictable cryptology  
3     keys, said data-processing system comprising:

4                 means for determining, for each of a plurality of evictable cryptology keys in a  
5     computer module, a replacement expense for each said evictable cryptology key, said  
6     replacement expense determined by:

7                     a probability that each said evictable cryptology key will be needed by  
8                     the computer module after said evictable cryptology key is evicted, and  
9                     an amount of cycle time required to re-store, if evicted, each said  
10                    evictable cryptology key in the computer module;

11                means for identifying a least expensive evictable cryptology key based on said  
12     replacement expense; and

13                means for replacing said least expensive evictable cryptology key with a  
14     replacement cryptology key.

15           7.     The data processing system of claim 6, said means for replacing said least  
16     expensive cryptology key further comprising:

17                means for locating a blob comprising said least expensive evictable cryptology  
18     key and a security software shell;

19                means for removing said security software shell from said blob; and

20                means for storing said least expensive evictable cryptology key in said computer  
21     module.

22           8.     The data processing system of claim 6 further comprising:

23                means for determining said cycle time by calculating a number of generations to  
24     a nearest ancestor of said least expensive evictable cryptology key, said nearest ancestor  
25     being from a plurality of non-evicted remaining cryptology keys in the computer module.

1           9.     The data processing system of claim 8 further comprising:

2                 means for storing, if a parent cryptology key of said least expensive evictable  
3 cryptology key is not stored in said computer module, a child cryptology key of said  
4 nearest ancestor key of said least expensive evictable cryptology key; and

5                 means for repeating said storing step until said least expensive evictable  
6 cryptology key is stored in said computer module.

1           10.    The data processing system of claim 6, wherein the computer module is a Trusted  
2 Platform Module (TPM).

2025-06-06 10:00:00

11. A computer usable medium for replacing a cryptology key in a computer module, wherein said computer module includes a plurality of evictable cryptology keys, said computer usable medium comprising:

computer program code for determining, for each of a plurality of evictable cryptology keys in a computer module, a replacement expense for each said evictable cryptology key, said replacement expense determined by:

a probability that each said evictable cryptology key will be needed by the computer module after said evictable cryptology key is evicted, and an amount of cycle time required to re-store, if evicted, each said evictable cryptology key in the computer module;

computer program code for identifying a least expensive evictable cryptology key based on said replacement expense; and

computer program code for replacing said least expensive evictable cryptology key with a replacement cryptology key.

12. The computer usable medium of claim 11, said computer program code for replacing said least expensive cryptology key further comprising:

computer program code for locating a blob comprising said least expensive evictable cryptology key and a security software shell;

computer program code for removing said security software shell from said blob;

and

computer program code storing said least expensive evictable cryptology key in said computer module.

1        13.    The computer usable medium of claim 11 further comprising:  
2                computer program code for determining said cycle time by calculating a number  
3 of generations to a nearest ancestor of said least expensive evictable cryptology key, said  
4 nearest ancestor being from a plurality of non-evicted remaining cryptology keys in the  
5 computer module.

1        14.    The computer usable medium of claim 13 further comprising:  
2                computer program code for storing, if a parent cryptology key of said least  
3 expensive evictable cryptology key is not stored in said computer module, a child  
4 cryptology key of said nearest ancestor key of said least expensive evictable cryptology  
5 key; and  
6                computer program code for repeating said storing step until said least expensive  
7 evictable cryptology key is stored in said computer module.

1        15.    The computer usable medium of claim 11, wherein the computer module is a  
2 Trusted Platform Module (TPM).